CS 2LC3
Logical Reasoning for Computer Science

Tutorial 5

Mahdee Jodayree

Habib Ben Abdallah

McMaster University

October 18th, 2022

Outline

- Announcements / Reminders
- Formal logic
- Quantification
- Universal quantification
- Existential quantification
- English to predicate logic

Announcements

- Midterm is on October 25th
- Sheet sheets is allowed for the midterm, one double sided page cheat sheet will be allowed. Dr. Janicki sent a notification from Mosaic.
- You can use a cheat sheet for the Axioms and theorems.
- Assignment 2 is now posted on the course website and it is due November 7 (Monday), 2022, 23:59 PM.

Slides that are important for the Midterm are the following.

- Post conditions and preconditions
- 7.2
- 8.3
- 9.4a
- 9.4 axiom
- 9.34
- 9.29

Post conditions and preconditions

From Tutorial 1

Hoare Triples (Assignment statement)

- Exercise 1.11

1.11 Using Definition (1.12) of the assignment statement on page 18, determine preconditions for the following statements and postconditions.

Statement	Postcondition	Precondition
$x := x - 1$	$x^2 + 2 \cdot x = 3$	
$x := x - 1$	$(x + 1) \cdot (x - 1) = 0$	
$y := x + y$	$y = x$	

Please see tutorial 1 for the solution

Formal logic

A *formal logical system*, or *logic*, is a set of rules defined in terms of

- a set of *symbols*,
- a set of *formulas* constructed from the symbols,
- a set of distinguished formulas called *axioms*, and
- a set of *inference rules*.

$$\frac{H_1, H_2, \ldots, H_n}{C}$$

where formulas $H_1, H_2, \ldots, H_n$ are the *premises* (or *hypotheses*) of the inference rule and formula C is its *conclusion*.

Consistent Logic.

(7.1) **Definition.** A logic is *consistent* if at least one of its formulas is a theorem and at least one is not; otherwise, the logic is *inconsistent.*

For example, logic **E** is consistent, because *true* is a theorem and *false* is not. Adding *false* $\equiv$ *true* as an axiom to **E** would make it inconsistent.

PQ-L Logic

PQ-L forcefully illustrates the view that a logic is a system for manipulating symbols, independent of meaning.

Below are three formulas of PQ-L.

– – – P – Q – –
P Q –
– P – Q – –

Below are three formulas of PQ-L.

– – – P – Q – –
P Q –
– P – Q – –

PQ-L uses the Hilbert style of proof. Here is a proof of theoremhood of – – – – P – – – Q – – – – – – – –. This theorem, together with the fact that – P – Q – is not a theorem, tells us that PQ-L is consistent.

– – – – P – – – Q – – – – – – –

1.	– P – Q – –	Axiom 0
2.	– – P – Q – – –	Axiom 1
3.	– – – P – – Q – – – – –	Inf. rule, 1, 2
4.	– – – – P – – – Q – – – – – – –	Inf. rule, 1, 3

Formal logic

(7.1) **Definition.** A logic is *consistent* if at least one of its formulas is a theorem and at least one is not; otherwise, the logic is *inconsistent*.

TABLE 7.1. LOGIC PQ–L

Symbols:	P, Q, –
Formulas:	Sequences of the form a P b Q c, where a, b, and c denote finite sequences of zero or more dashes –.
Axioms:	0 : – P – Q – – 1 : – – P – Q – – –
Inference Rule:	$\dfrac{a\ \mathrm{P}\ b\ \mathrm{Q}\ c,\quad d\ \mathrm{P}\ e\ \mathrm{Q}\ f}{a\ d\ \mathrm{P}\ b\ e\ \mathrm{Q}\ c\ f}$

(7.2) **Addition-equality Interpretation.** A formula a P b Q c is mapped to $\#a + \#b = \#c$, where $\#x$ denotes the number of dashes in sequence x.

For example, formulas – P Q – and – P – – Q – – – are mapped to $1 + 0 = 1$ and $1 + 2 = 3$, which are *true*, and – P – Q – is mapped to $1 + 1 = 1$, which is *false*. Also, axiom – P – Q – – of PQ-L is interpreted as $1 + 1 = 2$ and axiom – – P – Q – – – as $2 + 1 = 3$.

Formal logic

(7.1) **Definition.** A logic is *consistent* if at least one of its formulas is a theorem and at least one is not; otherwise, the logic is *inconsistent*.

TABLE 7.1. LOGIC PQ–L

Symbols:	P, Q, –
Formulas:	Sequences of the form a P b Q c, where a, b, and c denote finite sequences of zero or more dashes –.
Axioms:	0 : – P – Q – – 1 : – – P – Q – – –
Inference Rule:	$\dfrac{a\ \mathrm{P}\ b\ \mathrm{Q}\ c,\ \ d\ \mathrm{P}\ e\ \mathrm{Q}\ f}{a\ d\ \mathrm{P}\ b\ e\ \mathrm{Q}\ c\ f}$

(7.2) **Addition-equality Interpretation.** A formula a P b Q c is mapped to $\#a + \#b = \#c$, where $\#x$ denotes the number of dashes in sequence x.

For example, formulas – P Q – and – P – – Q – – – are mapped to $1 + 0 = 1$ and $1 + 2 = 3$, which are *true*, and – P – Q – is mapped to $1 + 1 = 1$, which is *false*. Also, axiom – P – Q – – of PQ-L is interpreted as $1 + 1 = 2$ and axiom – – P – Q – – – as $2 + 1 = 3$.

Formal logic

(7.5) **Definition.** Let S be a set of interpretations for a logic and F be a formula of the logic. F is *satisfiable* (under S) iff at least one interpretation of S maps F to *true*. F is *valid* (under S) iff every interpretation in S maps F to *true*.

An interpretation is a model for a logic iff every theorem is mapped to *true* by the interpretation.

(7.6) **Definition.** A logic is *sound* iff every theorem is valid. A logic is *complete* iff every valid formula is a theorem.

Sound and complete logic.

A sound and complete logic allows exactly the valid formulas to be proved. Failure to prove that a formula is a theorem in such a logic cannot be attributed to weakness of the logic. Unfortunately, many domains of discourse of concern to us —arithmetic truths, program behavior, and so on— do not have sound and complete axiomatizations. This is a consequence of Gödel's incompleteness theorem (see Historical note 7.1), which states that no formal logical system that axiomatizes arithmetic can be both sound and complete. Fortunately, this incompleteness is not a problem in practice.

Formal logic

7.1 Give a finite set of axioms that can be added to PQ-L to make it sound and complete under Addition-Equality Interpretation (7.2).

7.1 Two axioms suffice:

(a) P – Q – (c) PQ

(b) – P Q –

This is because any valid formula is equivalent to $x + y = z$ and, by arithmetic, this is equivalent to $(1 + 1 + \cdots + 1) + (1 + 1 + \cdots + 1) = (1 + 1 + 1 \cdots)$ where the first sum has x 1's, the second sum has y 1's and the RHS has $x + y$ 1's. Thus, $x + y = z$ can be proved by invoking the PQ-L inference rule along with x instances of (a) and y instances of (b).

Axiom (c) PQ is interpreted as 0+0=0 makes PQ-L sound and complete under the addition-equality interpretation

Formal logic

7.2 Consider the logic defined as follows, where a, b, and c denote finite sequences of zero or more o's.

Symbols: M, I, o
Formulas: Sequences of the form a M b I c
Axiom: ooMooIoooo

Inference Rule R1:
$$\frac{a\ \mathrm{M}\ b\ \mathrm{I}\ c}{a\ a\ \mathrm{M}\ b\ \mathrm{I}\ c\ c}$$

Inference Rule R2:
$$\frac{a\ \mathrm{M}\ b\ b\ \mathrm{I}\ c\ c}{a\ a\ \mathrm{M}\ b\ \mathrm{I}\ c\ c}$$

(a) Give 5 formulas of this logic.
(b) State and prove five theorems of the logic.
(c) Give an interpretation of the logic that makes multiplication of integers a model.
(d) Give a formula that is *true* according to your interpretation but is not a theorem. Argue (informally) why it cannot be a theorem.

7.2 Consider the logic defined as follows, where a, b, and c denote finite sequences of zero or more o's.

Symbols: M, I, o
Formulas: Sequences of the form a M b I c
Axiom: ooMooIoooo

Inference Rule R1:
$$\frac{a\ \mathrm{M}\ b\ \mathrm{I}\ c}{a\ a\ \mathrm{M}\ b\ \mathrm{I}\ c\ c}$$

Inference Rule R2:
$$\frac{a\ \mathrm{M}\ b\ b\ \mathrm{I}\ c\ c}{a\ a\ \mathrm{M}\ b\ \mathrm{I}\ c\ c}$$

(a) Give 5 formulas of this logic.

(i) oMoIo (ii) ooMoIoo (iii) oMooIoo (iv) MI (v) ooooMooIo

7.2 Consider the logic defined as follows, where a, b, and c denote finite sequences of zero or more o's.

Symbols: M, I, o
Formulas: Sequences of the form a M b I c
Axiom: ooMooIoooo

Inference Rule R1:
$$\frac{a\ \mathrm{M}\ b\ \mathrm{I}\ c}{a\ a\ \mathrm{M}\ b\ \mathrm{I}\ c\ c}$$

Inference Rule R2:
$$\frac{a\ \mathrm{M}\ b\ b\ \mathrm{I}\ c\ c}{a\ a\ \mathrm{M}\ b\ \mathrm{I}\ c\ c}$$

(b) State and prove five theorems of the logic.

The textbook solution is incorrect:
The authors made an error.
The rules are not symmetric, there is no way to shorten a sequence before M.
To prove 3 one need a rule
R3: aaMbIcc/aMbbIc
which is symmetric to R2,
or an axiom oMoIo. (i.e, 1x1=1)

7.2 Consider the logic defined as follows, where a, b, and c denote finite sequences of zero or more o's.

Symbols: M, I, o
Formulas: Sequences of the form a M b I c
Axiom: ooMooIoooo

Inference Rule R1: $$\frac{a\ \mathrm{M}\ b\ \mathrm{I}\ c}{a\ a\ \mathrm{M}\ b\ \mathrm{I}\ c\ c}$$

Inference Rule R2: $$\frac{a\ \mathrm{M}\ b\ b\ \mathrm{I}\ c\ c}{a\ a\ \mathrm{M}\ b\ \mathrm{I}\ c\ c}$$

(b) State and prove five theorems of the logic.

The textbook solution is incorrect:
The authors made an error.
The rules are not symmetric, there is no way to shorten
a sequence before M.
To prove 3 one need a rule
R3: aaMbIcc/aMbbIc
which is symmetric to R2,
or an axiom oMoIo. (i.e, 1x1=1)

Every line of a proof is a theorem, so the following proof contains 5 theorems.

ooooMooooIooooooooooooooo

1. ooMooIoooo — Axiom
2. ooooMooIooooooooo — $R1$, 1

3. ooooMoIoooo — R2, 1

You cannot apply R2 to 3 as we have only one 'o' between M and I, we can only apply R1, so

4. oooooooMoIooooooooo — R1, 3

we can apply only R1 so we get

5. ooooooooooooooooMoIooooooooooooooooo — R1, 3
6. oooooooMoIooooooooo — R2, 2

7.2 Consider the logic defined as follows, where a, b, and c denote finite sequences of zero or more o's.

Symbols: M, I, o
Formulas: Sequences of the form $a\ \mathrm{M}\ b\ \mathrm{I}\ c$
Axiom: ooMooIoooo

Inference Rule R1:
$$\frac{a\ \mathrm{M}\ b\ \mathrm{I}\ c}{a\ a\ \mathrm{M}\ b\ \mathrm{I}\ c\ c}$$

Inference Rule R2:
$$\frac{a\ \mathrm{M}\ b\ b\ \mathrm{I}\ c\ c}{a\ a\ \mathrm{M}\ b\ \mathrm{I}\ c\ c}$$

(c) Give an interpretation of the logic that makes multiplication of integers a model.

Let a sequence of x o's denote the integer x. Symbol "M" denotes "multiplied by" and Symbol "I" denotes "equals" so that, for example, ooMooooIoooooooo is interpreted as $2 \cdot 4 = 8$.

2 . 4 = 8

7.2 Consider the logic defined as follows, where a, b, and c denote finite sequences of zero or more o's.

Symbols: M, I, o
Formulas: Sequences of the form a M b I c
Axiom: ooMooIoooo

Inference Rule R1:
$$\frac{a\ \mathrm{M}\ b\ \mathrm{I}\ c}{a\ a\ \mathrm{M}\ b\ \mathrm{I}\ c\ c}$$

Inference Rule R2:
$$\frac{a\ \mathrm{M}\ b\ b\ \mathrm{I}\ c\ c}{a\ a\ \mathrm{M}\ b\ \mathrm{I}\ c\ c}$$

(d) Give a formula that is *true* according to your interpretation but is not a theorem. Argue (informally) why it cannot be a theorem.

Valid but not provable: oooMoIooo. Each inference rule doubles either the value before the M or the value after the M. The axiom has 2 o's before the M and 2 after. There is no way by doubling 2 to reach 3 or 1, so oooMoIooo is not provable.

Formal logic

7.5 This exercise concerns a new calculus, the $01\diamond$-calculus . The symbols of the calculus are

- Variables x , y , z , ...
- The three constant symbols 0 , 1 , and $\diamond$.
- The binary infix predicate symbol $=$.
- Parentheses.

Formulas of the calculus have the form $\alpha = \beta$, where α and β are sequences of one or more constants, possibly with balanced parentheses as usual to indicate aggregation. Examples of expressions are

$$0\diamond = 1 \quad \text{and} \quad (\diamond x)(\diamond\diamond) = 10 \quad .$$

By definition, if parentheses are omitted, left association is assumed, so that 0100 is shorthand for $((01)0)0$.

The $01\diamond$-calculus has inference rules Leibniz, Substitution, and Transitivity of equality $=$. *Note that symmetry and reflexivity of* $=$ *are not axioms*, so be extremely careful in applying inference rules. There are four axioms:

Left zero:	$0\diamond = 1$
Zero:	$x0\diamond = x1$
Left one:	$1\diamond = 10$
One:	$x1\diamond = x \diamond 0$

Formal logic

A *theorem* of the calculus is either an axiom or an expression $X = Y$ such that X can be transformed into Y using the inference rules. As an example, we prove that $011 \diamond 0 = 1000$ is a theorem.

$$
\begin{array}{ll}
 & 011 \diamond 0 \\
= & \quad \langle \text{Axiom One, with } x := 01 \rangle \\
 & 01 \diamond 00 \\
= & \quad \langle \text{Axiom One, with } x := 0 \rangle \\
 & 0 \diamond 000 \\
= & \quad \langle \text{Axiom Left zero} \rangle \\
 & 1000
\end{array}
$$

We now give meaning to the $01\diamond$-calculus by defining interpretations for it. A *state* assigns to each variable a natural number or $\diamond$. For example, the state $\{(x, 19), (y, \diamond)\}$ assigns 19 to z and $\diamond$ to y. Expressions are evaluated in a state by first replacing each variable by its value in the state and then applying the following rules. (In the rules, $x \succ y$ means that x evaluates to y).

$m\,n \succ (2 \cdot m + n)$	(for integers m and n)
$m \diamond \succ (m + 1)$	(for integer m)
$\diamond n \succ (2 + n)$	(for integer n)
$\diamond\diamond \succ 2$	
$(x = x) \succ \mathit{true}$	(for x an integer)
$(x = y) \succ \mathit{false}$	(for x and y different integers)

Formal logic

(a) Prove: $0 \diamond \diamond = 10$.
(b) Prove: $0 \diamond \diamond\diamond = 11$.

(i) Evaluate the expression $1011 \diamond \diamond$ in the state $\{(x, 19), (y, \diamond)\}$.
(j) Evaluate the expression $1x0y\diamond$ in the state $\{(x, 19), (y, \diamond)\}$.

(m) Show that the $01\diamond$-calculus with the interpretation given above is sound by checking that all four axioms are valid and that all three inference rules preserve validity.
(n) Show that the $01\diamond$-calculus is incomplete by finding a valid expression that is not a theorem.
(o) Show that the expression $x1 = \diamond\diamond$ is unsatisfiable.

Formal logic

7.5 (a)

$$
\begin{aligned}
& 0 \diamond \diamond \\
= \quad & \langle \text{Left zero} \rangle \\
& 1 \diamond \\
= \quad & \langle \text{Left one} \rangle \\
& 10
\end{aligned}
$$

(b)

$$
\begin{aligned}
& 0 \diamond \diamond \diamond \\
= \quad & \langle \text{Part (a) of the exercise} \rangle \\
& 10 \diamond \\
= \quad & \langle \text{Zero, with } x := 1 \rangle \\
& 11
\end{aligned}
$$

Formal logic

(i) Evaluate the expression $1011 \diamond \diamond$ in the state $\{(x, 19), (y, \diamond)\}$.

$$
\begin{array}{ll}
 & (((((1)0)1)1)\diamond)\diamond \\
\succ & \quad \langle \text{Part (h) of this exercise} \rangle \\
 & (12)\diamond \\
\succ & \quad \langle \text{Evaluation rule } m\diamond \succ m+1 \rangle \\
 & 13
\end{array}
$$

(j) Evaluate the expression $1x0y\diamond$ in the state $\{(x, 19), (y, \diamond)\}$.

$$
\begin{array}{ll}
 & (((((1)x)0)y)\diamond)[x, y := 19, \diamond] \\
\succ & \quad \langle \text{Textual substitution} \rangle \\
 & ((((1)(19))0)\diamond)\diamond \\
\succ & \quad \langle \text{Evaluation rule } mn \succ 2 \cdot m + n \rangle \\
 & (((21)0)\diamond)\diamond \\
\succ & \quad \langle \text{Evaluation rule } mn \succ 2 \cdot m + n \rangle \\
 & ((42)\diamond)\diamond \\
\succ & \quad \langle \text{Evaluation rule } m\diamond \succ m+1 \rangle \\
 & (43)\diamond \\
\succ & \quad \langle \text{Evaluation rule } m\diamond \succ m+1 \rangle \\
 & 44
\end{array}
$$

Formal logic

(m) We show that $x0\diamond = x1$ is valid, we evaluate it under the two possiblities for x: x is an integer m and x is a $\diamond$.

$$
\begin{array}{ll}
 & m0\diamond = m1 \\
\succ & \quad \langle \text{Evaluation rule } mn = 2\cdot m + n \text{, twice} \rangle \\
 & (2\cdot m)\diamond = (2\cdot m + 1) \\
\succ & \quad \langle \text{Evaluation rule } m\diamond \succ (m+1) \rangle \\
 & (2\cdot m + 1) = (2\cdot m + 1) \\
\succ & \quad \langle \text{Evaluation rule } x = x \succ \mathit{true} \rangle \\
 & \mathit{true}
\end{array}
$$

$$
\begin{array}{ll}
 & \diamond 0\diamond = \diamond 1 \\
\succ & \quad \langle \text{Evaluation rule } \diamond n \succ (2+n) \text{, twice} \rangle \\
 & 2\diamond = 3 \\
\succ & \quad \langle \text{Evaluation rule } m\diamond \succ (m+1) \rangle \\
 & 3 = 3 \\
\succ & \quad \langle \text{Evaluation rule } x = x \succ \mathit{true} \rangle \\
 & \mathit{true}
\end{array}
$$

Follow the same reasoning for the other axioms.

Formal logic

(n) The expression $1 = 1$ is a not a theorem because it does not have $\diamond$ in its LHS. That it is valid is a direct consequence of evaluation rule $x = x \succ \mathit{true}$.

(o) Show that the expression $x1 = \diamond\diamond$ is unsatisfiable. For x any integer m, we have,

$$
\begin{array}{ll}
 & m1 = \diamond\diamond \\
\succ & \quad \langle \text{Evaluation rules } mn = 2\cdot m + n \text{ and } \diamond\diamond \succ 2 \rangle \\
 & 2\cdot m + 1 = 2 \\
\succ & \quad \langle \text{The LHS is odd and the RHS is even} \rangle \\
 & \mathit{false}
\end{array}
$$

Hence, in any state the expression is *false* and is therefore unsatisfiable.

When x=square, perform the steps.

SYNTAX AND INTERPRETATION OF QUANTIFICATION

Here are examples of quantifications, assuming, as we do throughout this chapter, that i has type $\mathbb{Z}$.

$$
\begin{array}{rcl}
(+i \mid 0 \le i < 4 : i \cdot 8) & = & 0 \cdot 8 \ + \ 1 \cdot 8 \ + \ 2 \cdot 8 \ + \ 3 \cdot 8 \\
(\cdot i \mid 0 \le i < 3 : i + (i+1)) & = & (0+1) \cdot (1+2) \cdot (2+3) \\
(\wedge i \mid 0 \le i < 2 : i \cdot d \neq 6) & \equiv & 0 \cdot d \neq 6 \ \wedge \ 1 \cdot d \neq 6 \\
(\vee i \mid 0 \le i < 21 : b[i] = 0) & \equiv & b[0] = 0 \ \vee \ \cdots \ \vee \ b[20] = 0
\end{array}
$$

Many notations are used for quantification. Different ways are used to express range R and body P, and, for operators $\vee$ and $\wedge$, the range is not given as a separate entity. For example, one sees the following.

$\Sigma_{i=1}^{n} x_i$	for	$(+i \mid 1 \leq i \leq n : x_i)$
$\forall i. 1 \leq i \Rightarrow x_i = 0$	for	$(\wedge i \mid 1 \leq i : x_i = 0)$
$(\forall i) 1 \leq i \Rightarrow x_i = 0$	for	$(\wedge i \mid 1 \leq i : x_i = 0)$
$\exists i \,.\, 1 \leq i \wedge x_i = 0$	for	$(\vee i \mid 1 \leq i : x_i = 0)$

We use the linear notation $(\star x \mid R : P)$ throughout, for all quantifications, but we will bow to convention and use a different symbol for $\star$ in certain cases. In particular, in Chaps. 9 and 15 we write

$(+x \mid R : P)$	as	$(\Sigma\, x \mid R : P)$
$(\cdot x \mid R : P)$	as	$(\Pi\, x \mid R : P)$
$(\vee x \mid R : P)$	as	$(\exists x \mid R : P)$
$(\wedge x \mid R : P)$	as	$(\forall x \mid R : P)$

Quantification

(8.1) $f : t_1 \times \cdots \times t_n \to r \quad .$

function	type	typical function application
plus	$\mathbb{Z} \times \mathbb{Z} \to \mathbb{Z}$	$plus(1,3)$ or $1+3$
not	$\mathbb{B} \to \mathbb{B}$	$not.true$ or $\neg true$
less	$\mathbb{Z} \times \mathbb{Z} \to \mathbb{B}$	$less(5,3)$ or $5<3$

Symmetry: $b \star c = c \star b$

Associativity: $(b \star c) \star d = b \star (c \star d)$

Identity u**:** $u \star b = b = b \star u$

Quantification

(8.6) $(\star x{:}t1, y{:}t2 \mid R : P)$

where:

- Variables x and y are distinct. They are called the *bound variables* or *dummies* of the quantification. There may be one or more dummies.
- $t1$ and $t2$ are the types of dummies x and y. If $t1$ and $t2$ are the same type, we may write $(\star x, y{:}t1 \mid R : P)$. In the interest of brevity, we usually omit the type when it is obvious from the context, writing simply $(\star x, y \mid R : P)$.
- R, a boolean expression, is the *range* of the quantification —values assumed by x and y satisfy R. R may refer to dummies x and y. If the range is omitted, as in $(\star x \mid : P)$, then the range *true* is meant.
- P, an expression, is the *body* of the quantification. P may refer to dummies x and y.
- The type of the result of the quantification is the type of P.

Expression $(\star x{:}X \mid R : P)$ denotes the application of operator $\star$ to the values P for all x in X for which range R is true[3].

Quantification

(8.11) Provided $\neg occurs(\text{`}y\text{'}, \text{`}x, F\text{'})$,

$$(\star y \mid R : P)[x := F] \;=\; (\star y \mid R[x := F] : P[x := F]) \quad .$$

$$(+i \mid 0 \leq i < n : b[i] = n)[n := m] \;=\; (+i \mid 0 \leq i < m : b[i] = m)$$
$$(+y \mid 0 \leq y < n : b[y] = n)[n := y] \;=\; (+j \mid 0 \leq j < y : b[j] = y)$$

(8.12) **Leibniz:**
$$\frac{P = Q}{(\star x \mid E[z := P] : S) = (\star x \mid E[z := Q] : S)}$$

$$\frac{R \;\Rightarrow\; P = Q}{(\star x \mid R : E[z := P]) = (\star x \mid R : E[z := Q])}$$

(8.13) **Axiom, Empty range:** $(\star x \mid \mathit{false} : P) \;=\; u$ (the identity of $\star$)

(8.14) **Axiom, One-point rule:** Provided $\neg occurs(\text{`}x\text{'}, \text{`}E\text{'})$,

$$(\star x \mid x = E : P) \;=\; P[x := E]$$

Quantification

(8.15) **Axiom, Distributivity:** Provided each quantification is defined,

$$(\star x \mid R : P) \star (\star x \mid R : Q) \;=\; (\star x \mid R : P \star Q) \quad .$$

(8.16) **Axiom, Range split:** Provided $R \wedge S \equiv \mathit{false}$ and each quantification is defined,

$$(\star x \mid R \vee S : P) \;=\; (\star x \mid R : P) \star (\star x \mid S : P)$$

(8.17) **Axiom, Range split:** Provided each quantification is defined,

$$(\star x \mid R \vee S : P) \star (\star x \mid R \wedge S : P) \;=\; (\star x \mid R : P) \star (\star x \mid S : P)$$

(8.18) **Axiom, Range split for idempotent $\star$:** Provided each quantification is defined,

$$(\star x \mid R \vee S : P) \;=\; (\star x \mid R : P) \star (\star x \mid S : P)$$

Quantification

(8.19) **Axiom, Interchange of dummies:** Provided each quantification is defined, $\neg occurs(\text{`}y\text{'}, \text{`}R\text{'})$ and $\neg occurs(\text{`}x\text{'}, \text{`}Q\text{'})$,

$$(\star x \mid R : (\star y \mid Q : P)) = (\star y \mid Q : (\star x \mid R : P))$$

(8.20) **Axiom, Nesting:** Provided $\neg occurs(\text{`}y\text{'}, \text{`}R\text{'})$,

$$(\star x, y \mid R \wedge Q : P) = (\star x \mid R : (\star y \mid Q : P))$$

(8.21) **Axiom, Dummy renaming:** Provided $\neg occurs(\text{`}y\text{'}, \text{`}R, P\text{'})$,

$$(\star x \mid R : P) = (\star y \mid R[x := y] : P[x := y])$$

Let f be a function that has an inverse f^{-1}, so that $x = f.y \equiv y = f^{-1}.x$. Then

(8.22) **Change of dummy:** Provided $\neg occurs(\text{`}y\text{'}, \text{`}R, P\text{'})$ and f has an inverse,

$$(\star x \mid R : P) = (\star y \mid R[x := f.y] : P[x := f.y])$$

Quantification

(8.23) **Theorem Split off term.** For $n{:}\mathbb{N}$ and dummies $i{:}\mathbb{N}$,

$$(\star i \mid 0 \le i < n+1 : P) = (\star i \mid 0 \le i < n : P) \star P[i := n]$$
$$(\star i \mid 0 \le i < n+1 : P) = P[i := 0] \star (\star i \mid 0 < i < n+1 : P) .$$

Quantification

8.1 Given are functions a, b, c, d, and e with types as follows.

$$a : A \to B$$
$$b : B \to C$$
$$c : C \to A$$
$$d : A \times C \to D$$
$$e : B \times B \to E$$

State whether each expression below is type correct. If not, explain why. Assume $u{:}A$, $w{:}B$, $x{:}C$, $y{:}D$, and $z{:}E$.

(b) $b.x$

(c) $e(a(c.x), a.u)$

Quantification

8.1 Given are functions a, b, c, d, and e with types as follows.

$$a : A \to B$$
$$b : B \to C$$
$$c : C \to A$$
$$d : A \times C \to D$$
$$e : B \times B \to E$$

State whether each expression below is type correct. If not, explain why. Assume $u{:}A$, $w{:}B$, $x{:}C$, $y{:}D$, and $z{:}E$.

(b) $b.x$
(c) $e(a(c.x), a.u)$

(b) Incorrect: argument to b must be of type B, but $x{:}C$.
(c) Type correct.

Midterm - Important

Quantification

8.3 Expand the following textual substitutions. If necessary, change the dummy, according to Dummy Renaming (8.21).

(a) $(\star x \mid 0 \leq x + r < n : x + v)[v := 3]$

(b) $(\star x \mid 0 \leq x + r < n : x + v)[x := 3]$

(8.21) **Axiom, Dummy renaming:** Provided $\neg occurs(\text{`}y\text{'}, \text{`}R, P\text{'})$,

$$(\star x \mid R : P) = (\star y \mid R[x := y] : P[x := y])$$

The "occurs" restrictions on these laws ensure that an expression that contains an occurrence of a dummy is not moved outside (or inside) the scope of that dummy.

We now generalize axiom Dummy renaming (8.21). We motivate this generalization as follows. Consider the expression

$$(+i \mid 2 \leq i \leq 10 : i^2) \quad .$$

Rewriting this expression so that the range starts at 0 instead of 2 yields the following expression.

$$(+k \mid 0 \leq k \leq 8 : (k+2)^2)$$

Here, note that the relationship between i and k is $i = k+2$, or $k = i-2$.

The equality of the two summations above is an instance of the following general theorem, which holds for *any* symmetric and associative binary operator $\star$. Let f be a function that has an inverse f^{-1} , so that $x = f.y \equiv y = f^{-1}.x$. Then

Quantification

8.3 Expand the following textual substitutions. If necessary, change the dummy, according to Dummy Renaming (8.21).

(a) $(\star x \mid 0 \leq x + r < n : x + v)[v := 3]$
(b) $(\star x \mid 0 \leq x + r < n : x + v)[x := 3]$

Solution:

$$\text{(a)}\quad (\star x \mid 0 \leq x + r < n : x + 3)$$

$$\text{(b)}\quad (\star x \mid 0 \leq x + r < n : x + v)$$

Quantification

8.3 Expand the following textual substitutions. If necessary, change the dummy, according to Dummy Renaming (8.21).

(d) $(\star x \mid 0 \leq x < r : (\star y \mid 0 \leq y : x + y + n))[n := x + y]$

Solution:

(d) $(\star z \mid 0 \leq z < r : (\star w \mid 0 \leq w : z + w + x + y))$

Quantification

8.5 Prove the following theorems. Provided $0 \leq n$,

(a) $(\Sigma i \mid 0 \leq i < n+1 : b[i]) = b[0] + (\Sigma i \mid 1 \leq i < n+1 : b[i])$

Quantification

8.5 Prove the following theorems. Provided $0 \leq n$,

(a) $(\Sigma\, i \mid 0 \leq i < n+1 : b[i]) \;=\; b[0] + (\Sigma\, i \mid 1 \leq i < n+1 : b[i])$

$$
\begin{array}{ll}
 & (\Sigma\, i \mid 0 \leq i < n+1 : b[i]) \\
= & \quad \langle (8.24), \text{ with } b, c, d := 0, 1, n+1 \rangle \\
 & (\Sigma\, i \mid 0 \leq i < 1 \;\vee\; 1 \leq i < n+1 : b[i]) \\
= & \quad \langle \text{Range split } (8.16) \rangle \\
 & (\Sigma\, i \mid 0 \leq i < 1 : b[i]) + (\Sigma\, i \mid 1 \leq i < n+1 : b[i]) \\
= & \quad \langle\, 0 \leq i < 1 \;\equiv\; i = 0 \,;\, \text{One-point rule } (8.14) \rangle \\
 & b[0] + (\Sigma\, i \mid 1 \leq i < n+1 : b[i])
\end{array}
$$

Quantification

8.6 Prove the following theorems. Provided $0 \leq n$,

(a) $(\vee i \mid 0 \leq i < n+1 : b[i] = 0) \equiv$
$(\vee i \mid 0 \leq i < n : b[i] = 0) \vee b[n] = 0$

(b) $(\wedge i \mid 0 \leq i < n+1 : b[i] = 0) \equiv$
$(\wedge i \mid 0 \leq i < n : b[i] = 0) \wedge b[n] = 0$

Quantification

8.6 Prove the following theorems. Provided $0 \leq n$,

(a) $(\vee i \mid 0 \leq i < n+1 : b[i] = 0) \equiv$
$(\vee i \mid 0 \leq i < n : b[i] = 0) \vee b[n] = 0$

(b) $(\wedge i \mid 0 \leq i < n+1 : b[i] = 0) \equiv$
$(\wedge i \mid 0 \leq i < n : b[i] = 0) \wedge b[n] = 0$

Quantification

8.6 The proofs of this exercise can be done in one step using Split off term (8.23). The proofs below do not make use of Split off term (8.23) and hence are longer.

(a)

$$
\begin{array}{ll}
 & (\forall i \mid 0 \le i < n+1 : b[i] = 0) \\
= & \quad \langle (8.24), \text{ with } b, c, d := 0, n, n+1 \rangle \\
 & (\forall i \mid 0 \le i < n \ \vee \ n \le i < n+1 : b[i] = 0) \\
= & \quad \langle \text{Range split (8.16)} \rangle \\
 & (\forall i \mid 0 \le i < n : b[i] = 0) \ \vee \ (\forall i \mid n \le i < n+1 : b[i] = 0) \\
= & \quad \langle \, n \le i < n+1 \ \equiv \ i = n \, ; \text{ One-point rule (8.14)} \rangle \\
 & (\forall i \mid 0 \le i < n : b[i] = 0) \ \vee \ b[n] = 0)
\end{array}
$$

(b)

$$
\begin{array}{ll}
 & (\wedge i \mid 0 \le i < n+1 : b[i] = 0) \\
= & \quad \langle (8.24), \text{ with } b, c, d := 0, n, n+1 \rangle \\
 & (\wedge i \mid 0 \le i < n \ \vee \ n \le i < n+1 : b[i] = 0) \\
= & \quad \langle \text{Range split (8.16)} \rangle \\
 & (\wedge i \mid 0 \le i < n : b[i] = 0) \ \wedge \ (\wedge i \mid n \le i < n+1 : b[i] = 0) \\
= & \quad \langle \, n \le i < n+1 \ \equiv \ i = n \, ; \text{ One-point rule (8.14)} \rangle \\
 & (\wedge i \mid 0 \le i < n : b[i] = 0) \ \wedge \ b[n] = 0)
\end{array}
$$

Universal quantification

$(\wedge x \mid R : P)$ is conventionally written as

(9.1) $(\forall x \mid R : P)$.

(9.2) **Axiom, Trading:** $(\forall x \mid R : P) \equiv (\forall x \mid : R \Rightarrow P)$

(9.5) **Axiom, Distributivity of $\vee$ over $\forall$:**

Provided $\neg occurs(\text{`}x\text{'}, \text{`}P\text{'})$,

$P \vee (\forall x \mid R : Q) \equiv (\forall x \mid R : P \vee Q)$

Universal quantification

Trading theorems for $\forall$

(9.3) **Trading:**

(a) $(\forall x \mid R : P) \equiv (\forall x \mid : \neg R \vee P)$

(b) $(\forall x \mid R : P) \equiv (\forall x \mid : R \wedge P \equiv R)$

(c) $(\forall x \mid R : P) \equiv (\forall x \mid : R \vee P \equiv P)$

(9.4) **Trading:**

(a) $(\forall x \mid Q \wedge R : P) \equiv (\forall x \mid Q : R \Rightarrow P)$

(b) $(\forall x \mid Q \wedge R : P) \equiv (\forall x \mid Q : \neg R \vee P)$

(c) $(\forall x \mid Q \wedge R : P) \equiv (\forall x \mid Q : R \wedge P \equiv R)$

(d) $(\forall x \mid Q \wedge R : P) \equiv (\forall x \mid Q : R \vee P \equiv P)$

Midterm - Important

(9.4) **Trading:**

(a) $(\forall x \mid Q \wedge R : P) \equiv (\forall x \mid Q : R \Rightarrow P)$

(b) $(\forall x \mid Q \wedge R : P) \equiv (\forall x \mid Q : \neg R \vee P)$

(c) $(\forall x \mid Q \wedge R : P) \equiv (\forall x \mid Q : R \wedge P \equiv R)$

(d) $(\forall x \mid Q \wedge R : P) \equiv (\forall x \mid Q : R \vee P \equiv P)$

Universal quantification

Additional theorems for $\forall$

(9.6) Provided $\neg occurs(\text{`}x\text{'}, \text{`}P\text{'})$,

$$(\forall x \mid R : P) \equiv P \vee (\forall x \mid : \neg R)$$

(9.7) **Distributivity of $\wedge$ over $\forall$:** Provided $\neg occurs(\text{`}x\text{'}, \text{`}P\text{'})$,

$$\neg(\forall x \mid : \neg R) \Rightarrow ((\forall x \mid R : P \wedge Q) \equiv P \wedge (\forall x \mid R : Q))$$

(9.8) $$(\forall x \mid R : true) \equiv true$$

(9.9) $$(\forall x \mid R : P \equiv Q) \Rightarrow ((\forall x \mid R : P) \equiv (\forall x \mid R : Q))$$

Universal quantification

Weakening, strengthening, and monotonicity for $\forall$

(9.10) **Range weakening/strengthening:**

$$(\forall x \mid Q \vee R : P) \Rightarrow (\forall x \mid Q : P)$$

(9.11) **Body weakening/strengthening:**

$$(\forall x \mid R : P \wedge Q) \Rightarrow (\forall x \mid R : P)$$

(9.12) **Monotonicity of $\forall$:**

$$(\forall x \mid R : Q \Rightarrow P) \Rightarrow ((\forall x \mid R : Q) \Rightarrow (\forall x \mid R : P))$$

Instantiation for $\forall$

(9.13) **Instantiation:** $(\forall x \mid : P) \Rightarrow P[x := E]$

Universal quantification

(9.4a).

$$
\begin{array}{ll}
 & (\forall x \mid Q \wedge R : P) \\
= & \quad \langle \text{Trading } (9.2) \rangle \\
 & (\forall x \mid : Q \wedge R \Rightarrow P) \\
= & \quad \langle \text{Shunting } (3.65) \rangle \\
 & (\forall x \mid : Q \Rightarrow (R \Rightarrow P)) \\
= & \quad \langle \text{Trading } (9.2) \rangle \\
 & (\forall x \mid Q : R \Rightarrow P)
\end{array}
$$

All other tradings consist on replacing P=>Q, with their expressions from Chapter 3, by using Leibniz (8.12).

Proof of (9.6), $(\forall x \mid R : P) \equiv P \vee (\forall x \mid : \neg R)$ (where x does not occur free in P).

$$
\begin{array}{ll}
 & (\forall x \mid R : P) \\
= & \quad \langle \text{Trading } (9.3) \rangle \\
 & (\forall x \mid : \neg R \vee P) \\
= & \quad \langle \vee \text{ distributes over } \forall \ (9.5) \rangle \\
 & P \vee (\forall x \mid : \neg R)
\end{array}
$$

Universal quantification

The proof of (9.7) uses
the technique of assuming the antecedent (see page 71). We assume the antecedent $\neg(\forall x \mid : \neg R)$ and prove the consequent:

$$
\begin{array}{ll}
 & (\forall x \mid R : P \wedge Q) \\
= & \quad \langle \text{Distributivity of } \forall \text{ over } \wedge \ (8.15) \rangle \\
 & (\forall x \mid R : P) \wedge (\forall x \mid R : Q) \\
= & \quad \langle (9.6) \text{ —since } \neg occurs(\text{`}x\text{'}, \text{`}P\text{'}) \rangle \\
 & (P \vee (\forall x \mid : \neg R)) \wedge (\forall x \mid R : Q) \\
= & \quad \langle \text{Assumption } \neg(\forall x \mid : \neg R) \text{, i.e. } (\forall x \mid : \neg R) \equiv false \rangle \\
 & (P \vee false) \wedge (\forall x \mid R : Q) \\
= & \quad \langle \text{Identity of } \vee \ (3.30) \rangle \\
 & P \wedge (\forall x \mid R : Q)
\end{array}
$$

Universal quantification

(9.8)

$$
\begin{array}{ll}
 & (\forall x \mid R : true) \\
= & \quad \langle \text{Trading (9.3)} \rangle \\
 & (\forall x \mid : \neg R \vee true) \\
= & \quad \langle \vee \text{ distributes over } \forall \text{ (9.5)} \rangle \\
 & true \vee (\forall x \mid : \neg R) \\
= & \quad \langle \text{Zero of } \vee \text{ (3.29)} \rangle \\
 & true
\end{array}
$$

(9.9)

$$
\begin{array}{ll}
 & (\forall x \mid R : P \equiv Q) \wedge (\forall x \mid R : P) \equiv \\
 & (\forall x \mid R : P \equiv Q) \wedge (\forall x \mid R : Q) \\
= & \quad \langle \forall \text{ distributes over } \wedge \text{ (8.15)} \rangle \\
 & (\forall x \mid R : (P \equiv Q) \wedge P) \equiv (\forall x \mid R : (P \equiv Q) \wedge Q) \\
= & \quad \langle (3.62),\ P \Rightarrow (Q \equiv R) \equiv P \wedge Q \equiv P \wedge R \rangle \\
 & (\forall x \mid R : P \wedge Q) \equiv (\forall x \mid R : P \wedge Q) \\
= & \quad \langle \text{Identity of } \equiv \text{ (3.3)} \rangle \\
 & true
\end{array}
$$

(9.10)

$$
\begin{array}{ll}
 & (\forall x \mid Q \vee R : P) \\
= & \quad \langle \text{Range split (8.18)} \rangle \\
 & (\forall x \mid Q : P) \wedge (\forall x \mid R : P) \\
\Rightarrow & \quad \langle \text{Strengthening (3.76b)} \rangle \\
 & (\forall x \mid Q : P)
\end{array}
$$

(9.11)

$$
\begin{array}{ll}
 & (\forall x \mid R : P \wedge Q) \\
= & \quad \langle \text{Distributivity of } \forall \text{ over } \wedge, \text{ (8.15)} \rangle \\
 & (\forall x \mid R : P) \wedge (\forall x \mid R : Q) \\
\Rightarrow & \quad \langle \text{Strengthening (3.76b)} \rangle \\
 & (\forall x \mid R : P)
\end{array}
$$

Universal quantification

Proof of Monotonicity of $\forall$ (9.12), $(\forall x \mid R : Q \Rightarrow P) \Rightarrow ((\forall x \mid R : Q) \Rightarrow (\forall x \mid R : P))$. Using shunting, we write (9.12) as $(\forall x \mid R : Q \Rightarrow P) \wedge (\forall x \mid R : Q) \Rightarrow (\forall x \mid R : P)$. We begin with the antecedent.

$$
\begin{array}{ll}
 & (\forall x \mid R : Q \Rightarrow P) \wedge (\forall x \mid R : Q) \\
= & \quad \langle \forall \text{ distributes over } \wedge, (8.15) \rangle \\
 & (\forall x \mid R : (Q \Rightarrow P) \wedge Q) \\
= & \quad \langle (3.66) \rangle \\
 & (\forall x \mid R : P \wedge Q) \\
\Rightarrow & \quad \langle \text{Body weakening } (9.11) \rangle \\
 & (\forall x \mid R : P)
\end{array}
$$

Universal quantification

Proof of Instantiation (9.13), $(\forall x \mid : P) \Rightarrow P[x := E]$. The introduction of the dummy that does not occur in P or E is necessary. For example, otherwise the theorem will not have been proved for the case $(\forall x \mid : x > 5) \Rightarrow (x > 5)[x := x]$, where the consequent equivales $x > 5$.

Let z be a variable that is not free in P or E.

$$
\begin{array}{ll}
 & (\forall x \mid : P) \\
= & \quad \langle \text{Dummy renaming (8.21)} — z \text{ is not free in } P \rangle \\
 & (\forall z \mid : P[x := z]) \\
\Rightarrow & \quad \langle \text{Range strengthening} — \mathit{true} \equiv \mathit{true} \vee z = E \rangle \\
 & (\forall z \mid z = E : P[x := z]) \\
= & \quad \langle \text{One-point rule} — z \text{ is not free in } E \rangle \\
 & P[x := z][z := E] \\
= & \quad \langle \text{Properties of textual substitution} — z \text{ is not free in } P \rangle \\
 & P[x := E]
\end{array}
$$

Existential quantification

Disjunction $\vee$ is symmetric and associative and has the identity *false*. Therefore, it is an instance of $\star$ of Sec. 8.2. The quantification $(\vee x \mid R : P)$ is typically written as

$$(\exists x \mid R : P) \quad .$$

The symbol $\exists$, which is read as "there exists", is called the *existential* quantifier. The expression is called an *existential quantification* and is read as "there exists an x in the range R such that P holds". A value $\hat{x}$ for which $(R \wedge P)[x := \hat{x}]$ is valid is called a *witness* for x in $(\exists x \mid R : P)$.

(9.17) **Axiom, Generalized De Morgan:**

$$(\exists x \mid R : P) \equiv \neg(\forall x \mid R : \neg P)$$

Existential quantification

Generalized De Morgan

(9.18) **Generalized De Morgan:** (a) $\neg(\exists x \mid R : \neg P) \equiv (\forall x \mid R : P)$

(b) $\neg(\exists x \mid R : P) \equiv (\forall x \mid R : \neg P)$

(c) $(\exists x \mid R : \neg P) \equiv \neg(\forall x \mid R : P)$

Trading theorems for $\exists$

(9.19) **Trading:** $(\exists x \mid R : P) \equiv (\exists x \mid : R \wedge P)$

(9.20) **Trading:** $(\exists x \mid Q \wedge R : P) \equiv (\exists x \mid Q : R \wedge P)$

Existential quantification

Additional theorems for $\exists$

(9.21) **Distributivity of $\wedge$ over $\exists$:** Provided $\neg occurs(\text{`}x\text{'}, \text{`}P\text{'})$,

$$P \wedge (\exists x \mid R : Q) \equiv (\exists x \mid R : P \wedge Q)$$

(9.22) Provided $\neg occurs(\text{`}x\text{'}, \text{`}P\text{'})$,

$$(\exists x \mid R : P) \equiv P \wedge (\exists x \mid : R)$$

(9.23) **Distributivity of $\vee$ over $\exists$:** Provided $\neg occurs(\text{`}x\text{'}, \text{`}P\text{'})$,

$$(\exists x \mid : R) \Rightarrow ((\exists x \mid R : P \vee Q) \equiv P \vee (\exists x \mid R : Q))$$

(9.24) $$(\exists x \mid R : false) \equiv false$$

Existential quantification

Weakening, strengthening, and monotonicity for $\exists$

(9.25) **Range weakening/strengthening:**

$$(\exists x \mid R : P) \Rightarrow (\exists x \mid Q \vee R : P)$$

(9.26) **Body weakening/strengthening:**

$$(\exists x \mid R : P) \Rightarrow (\exists x \mid R : P \vee Q)$$

(9.27) **Monotonicity of $\exists$:**

$$(\forall x \mid R : Q \Rightarrow P) \Rightarrow ((\exists x \mid R : Q) \Rightarrow (\exists x \mid R : P))$$

Existential quantification

Weakening, strengthening, and monotonicity for $\exists$

(9.25) **Range weakening/strengthening:**

$$(\exists x \mid R : P) \Rightarrow (\exists x \mid Q \vee R : P)$$

(9.26) **Body weakening/strengthening:**

$$(\exists x \mid R : P) \Rightarrow (\exists x \mid R : P \vee Q)$$

(9.27) **Monotonicity of $\exists$:**

$$(\forall x \mid R : Q \Rightarrow P) \Rightarrow ((\exists x \mid R : Q) \Rightarrow (\exists x \mid R : P))$$

Existential quantification

Introduction and interchange for $\exists$

(9.28) **$\exists$-Introduction:** $P[x := E] \Rightarrow (\exists x \mid : P)$

(9.29) **Interchange of quantifications:**

Provided $\neg occurs(\text{`}y\text{'}, \text{`}R\text{'})$ and $\neg occurs(\text{`}x\text{'}, \text{`}Q\text{'})$,

$$(\exists x \mid R : (\forall y \mid Q : P)) \Rightarrow (\forall y \mid Q : (\exists x \mid R : P))$$

Midterm - Important

Existential quantification

(9.30) **Metatheorem Witness.** Suppose $\neg occurs(\text{`}\hat{x}\text{'}, \text{`}P, Q, R\text{'})$. Then

$(\exists x \mid R : P) \Rightarrow Q$ is a theorem iff

$(R \wedge P)[x := \hat{x}] \Rightarrow Q$ is a theorem.

Identifier $\hat{x}$ is called a *witness* for the existential quantification. [1]

Existential quantification

(9.18a)

$$
\begin{array}{ll}
 & \neg(\exists x \mid R : \neg P) \\
= & \quad \langle \text{Generalized De Morgan (9.17), with } P := \neg P \rangle \\
 & \neg\neg(\forall x \mid R : \neg\neg P) \\
= & \quad \langle \text{Double negation (3.12), twice} \rangle \\
 & (\forall x \mid R : P)
\end{array}
$$

Proof of Generalized De Morgan (9.18b), $\neg(\exists x \mid R : P) \equiv (\forall x \mid R : \neg P)$.

$$
\begin{array}{ll}
 & \neg(\exists x \mid R : P) \\
= & \quad \langle \text{Generalized De Morgan (9.17)} \rangle \\
 & \neg\neg(\forall x \mid R : \neg P) \\
= & \quad \langle \text{Double negation (3.12)} \rangle \\
 & (\forall x \mid R : \neg P)
\end{array}
$$

Proof of Generalized De Morgan (9.18c), $(\exists x \mid R : \neg P) \equiv \neg(\forall x \mid R : P)$.

$$
\begin{array}{ll}
 & (\exists x \mid R : \neg P) \\
= & \quad \langle \text{Generalized De Morgan (9.17)} \rangle \\
 & \neg(\forall x \mid R : \neg\neg P) \\
= & \quad \langle \text{Double negation (3.12)} \rangle \\
 & \neg(\forall x \mid R : P)
\end{array}
$$

Existential quantification

Proof of Trading (9.19), $(\exists x \mid R : P) \equiv (\exists x \mid : R \wedge P)$.

$$
\begin{array}{ll}
 & (\exists x \mid R : P) \\
= & \quad \langle \text{De Morgan (9.17)} \rangle \\
 & \neg(\forall x \mid R : \neg P) \\
= & \quad \langle \text{Trading (9.3)} \rangle \\
 & \neg(\forall x \mid : \neg R \vee \neg P) \\
= & \quad \langle \text{De Morgan (3.47a)} \rangle \\
 & \neg(\forall x \mid : \neg(R \wedge P)) \\
= & \quad \langle \text{De Morgan (9.17)} \rangle \\
 & (\exists x \mid : R \wedge P)
\end{array}
$$

Existential quantification

Proof of Distributivity of $\wedge$ over $\exists$ (9.21), $P \wedge (\exists x \mid R : Q) \equiv (\exists x \mid R : P \wedge Q)$ (where x does not occur free in P).

$$
\begin{array}{ll}
 & (\exists x \mid R : P \wedge Q) \\
= & \quad \langle \text{De Morgan (9.17)} \rangle \\
 & \neg(\forall x \mid R : \neg(P \wedge Q)) \\
= & \quad \langle \text{De Morgan (3.47a)} \rangle \\
 & \neg(\forall x \mid R : \neg P \vee \neg Q) \\
= & \quad \langle \vee \text{ distributes over } \forall \text{ (9.5)} \rangle \\
 & \neg(\neg P \vee (\forall x \mid R : \neg Q)) \\
= & \quad \langle \text{Generalized De Morgan (9.18b)} \rangle \\
 & \neg(\neg P \vee \neg(\exists x \mid R : Q)) \\
= & \quad \langle \text{De Morgan (3.47a); Double negation (3.12)} \rangle \\
 & P \wedge (\exists x \mid R : Q)
\end{array}
$$

Existential quantification

Proof of (9.22), $(\exists x \mid R : P) \equiv P \wedge (\exists x \mid : R)$ (where x does not occur free in P).

$$
\begin{array}{ll}
 & (\exists x \mid R : P) \\
= & \quad \langle \text{Trading (9.19)} \rangle \\
 & (\exists x \mid : R \wedge P) \\
= & \quad \langle \wedge \text{ distributes over } \exists, \text{ (9.21)} \rangle \\
 & P \wedge (\exists x \mid : R)
\end{array}
$$

Proof of Distributivity of $\vee$ over $\exists$ (9.23), $(\exists x \mid : R) \Rightarrow ((\exists x \mid R : P \vee Q) \equiv P \vee (\exists x \mid R : Q))$ (where x does not occur free in P). We assume antecedent $(\exists x \mid : R)$ and prove the consequent.

$$
\begin{array}{ll}
 & (\exists x \mid R : P \vee Q) \\
= & \quad \langle \exists \text{ distributes over } \vee, \text{ (8.15)} \rangle \\
 & (\exists x \mid R : P) \vee (\exists x \mid R : Q) \\
= & \quad \langle (9.22),\ (\exists x \mid R : P) \equiv P \wedge (\exists x \mid : R) \rangle \\
 & (P \wedge (\exists x \mid : R)) \vee (\exists x \mid R : Q) \\
= & \quad \langle \text{Assumption } (\exists x \mid : R) \rangle \\
 & (P \wedge \mathit{true}) \vee (\exists x \mid R : Q) \\
= & \quad \langle \text{Identity of and (3.39)} \rangle \\
 & P \vee (\exists x \mid R : Q)
\end{array}
$$

Existential quantification

Proof of (9.24), $(\exists x \mid R : false) \equiv false$.

$$
\begin{array}{ll}
 & (\exists x \mid R : false) \\
= & \quad \langle \text{De Morgan (9.17)} \rangle \\
 & \neg(\forall x \mid R : \neg false) \\
= & \quad \langle \text{Negation of } false \ (3.13) \rangle \\
 & \neg(\forall x \mid R : true) \\
= & \quad \langle (9.8),\ (\forall x \mid R : true) \equiv true \text{ ; Definition of } false \ (3.8) \rangle \\
 & false
\end{array}
$$

9.23 Proof of Range weakening (9.25), $(\exists x \mid R : P) \Rightarrow (\exists x \mid Q \vee R : P)$.

$$
\begin{array}{ll}
 & (\exists x \mid Q \vee R : P) \\
= & \quad \langle \text{Range split (8.18)} \rangle \\
 & (\exists x \mid Q : P) \vee (\exists x \mid R : P) \\
\Leftarrow & \quad \langle \text{Weakening (3.76a)} \rangle \\
 & (\exists x \mid R : P)
\end{array}
$$

9.24 Proof of Body weakening (9.26), $(\exists x \mid R : P) \Rightarrow (\exists x \mid R : P \vee Q)$.

$$
\begin{array}{ll}
 & (\exists x \mid R : P \vee Q) \\
= & \quad \langle \exists \text{ distributes over } \vee, (8.15) \rangle \\
 & (\exists x \mid R : P) \vee (\exists x \mid R : Q) \\
\Leftarrow & \quad \langle \text{Weakening (3.76a)} \rangle \\
 & (\exists x \mid R : P)
\end{array}
$$

Existential quantification

Proof of Monotonicity of $\exists$ (9.27), $(\forall x \mid R : Q \Rightarrow P) \Rightarrow ((\exists x \mid R : Q) \Rightarrow (\exists x \mid R : P))$.

$$
\begin{array}{ll}
 & (\exists x \mid R : Q) \Rightarrow (\exists x \mid R : P) \\
= & \quad \langle \text{Contrapositive (3.61); De Morgan (9.18b), twice} \rangle \\
 & (\forall x \mid R : \neg P) \Rightarrow (\forall x \mid R : \neg Q) \\
\Leftarrow & \quad \langle \text{Monotonicity of } \forall \text{ (9.12), with } P, Q := \neg Q, \neg P \rangle
\end{array}
$$

$$
\begin{array}{ll}
 & (\forall x \mid R : \neg P \Rightarrow \neg Q) \\
= & \quad \langle \text{Contrapositive (3.61)} \rangle \\
 & (\forall x \mid R : Q \Rightarrow P)
\end{array}
$$

Proof of $\exists$-introduction (9.28), $P[x := E] \Rightarrow (\exists x \mid : P)$.

$$
\begin{array}{ll}
 & P[x := E] \Rightarrow (\exists x \mid : P) \\
= & \quad \langle \text{Contrapositive (3.61)} \rangle \\
 & \neg(\exists x \mid : P) \Rightarrow \neg P[x := E] \\
= & \quad \langle \text{De Morgan (9.18)b} \rangle \\
 & (\forall x \mid : \neg P) \Rightarrow \neg P[x := E] \\
= & \quad \langle \text{Property of textual substitution} \rangle \\
 & (\forall x \mid : \neg P) \Rightarrow (\neg P)[x := E] \\
= & \quad \langle \text{Instantiation (9.13),with } P := \neg P \rangle \\
 & \mathit{true}
\end{array}
$$

Existential quantification

(9.29)

$$
\begin{array}{ll}
 & (\exists x \mid : (\forall y \mid : P)) \;\Rightarrow\; (\forall y \mid : (\exists x \mid : P)) \\
= & \quad \langle \text{Implication (3.57), } p \Rightarrow q \;\equiv\; p \vee q \;\equiv\; q \,, \\
 & \quad \text{to eliminate the problematic } \Rightarrow \rangle \\
 & (\exists x \mid : (\forall y \mid : P)) \vee (\forall y \mid : (\exists x \mid : P)) \;\equiv\; (\forall y \mid : (\exists x \mid : P)) \\
= & \quad \langle \text{Distributivity of } \vee \text{ over } \forall \text{ (9.5) —so that the LHS} \\
 & \quad \text{and RHS have the same outer quantification} \rangle \\
 & (\forall y \mid : (\exists x \mid : (\forall y \mid : P)) \vee (\exists x \mid : P)) \;\equiv\; (\forall y \mid : (\exists x \mid : P)) \\
= & \quad \langle \text{Distributivity (8.15) —so that the LHS} \\
 & \quad \text{and RHS have the same two outer quantifications} \rangle \\
 & (\forall y \mid : (\exists x \mid : (\forall y \mid : P) \vee P)) \;\equiv\; (\forall y \mid : (\exists x \mid : P)) \\
= & \quad \langle \text{Instantiation (9.13) says } (\forall y \mid : P) \Rightarrow P \,, \\
 & \quad \text{which by (3.57) is equivalent to } (\forall y \mid : P) \vee P \;\equiv\; P \rangle \\
 & (\forall y \mid : (\exists x \mid : P)) \;\equiv\; (\forall y \mid : (\exists x \mid : P)) \quad \text{—Reflexivity of equality}
\end{array}
$$

Existential quantification

Proof. (9.30) $(\exists x \mid R : P) \Rightarrow Q$

$$
\begin{array}{ll}
= & \langle \text{Trading (9.19)} \rangle \\
& (\exists x \mid : R \wedge P) \Rightarrow Q \\
= & \langle \text{Implication (3.59); De Morgan (9.18b)} \rangle \\
& (\forall x \mid : \neg(R \wedge P)) \vee Q \\
= & \langle \text{Dummy renaming (8.21)}, -\!\!- \neg occurs(\text{`}\hat{x}\text{'}, \text{`}P, R\text{'}) \rangle \\
& (\forall \hat{x} \mid : \neg(R \wedge P)[x := \hat{x}]) \vee Q \\
= & \langle \text{Distributivity of } \vee \text{ over } \forall \text{ (9.5)} -\!\!- \neg occurs(\text{`}\hat{x}\text{'}, \text{`}Q\text{'}) \rangle \\
& (\forall \hat{x} \mid : \neg(R \wedge P)[x := \hat{x}] \vee Q) \\
= & \langle \text{Implication (3.59)} \rangle \\
& (\forall \hat{x} \mid : (R \wedge P)[x := \hat{x}] \Rightarrow Q)
\end{array}
$$

By Metatheorem (9.16), the last line is a theorem iff $(R \wedge P)[x := \hat{x}] \Rightarrow Q$ is a theorem. □

Midterm - Important

English to predicate logic

9.34 Formalize the following English sentences in predicate logic.

(c) Everybody loves everybody.

(d) Nobody loves everybody.

(e) Somebody loves nobody.

Midterm - Important

English to predicate logic

9.34 Formalize the following English sentences in predicate logic.

(c) Everybody loves everybody.

(d) Nobody loves everybody.

(e) Somebody loves nobody.

Hint:

Define $loves\ (x,y)$: $Person\ x\ loves\ person\ y.$

Let P be the set of all people.

∀ Every body

∃ Somebody

¬∃ Nobody

Midterm - Important

English to predicate logic

9.34 Formalize the following English sentences in predicate logic.

(c) Everybody loves everybody.

(d) Nobody loves everybody.

(e) Somebody loves nobody.

9.34 Define

$$loves(x, y): \text{ person } x \text{ loves person } y.$$

Let P be the set of all people.

(c) $(\forall x{:}P \mid{:} (\forall y{:}P \mid{:} loves(x, y)))$

(d) $\neg(\exists x{:}P \mid{:} (\forall y{:}P \mid{:} loves(x, y)))$

(e) $(\exists x{:}P \mid{:} \neg(\exists y{:}P \mid{:} loves(x, y)))$

English to predicate logic

9.29 Translate the following English statements into predicate logic.

(a) The natural number 1 is the only natural number that is smaller than positive integer p and divides p.

(c) Adding two odd integers yields an even number. (Use only addition and multiplication; do not use division, mod, or predicates $even.x$ and $odd.x$.)

English to predicate logic

9.29 Translate the following English statements into predicate logic.

(a) The natural number 1 is the only natural number that is smaller than positive integer p and divides p.

(c) Adding two odd integers yields an even number. (Use only addition and multiplication; do not use division, mod, or predicates $even.x$ and $odd.x$.)

(a) $(\forall d \mid 1 < d < p : \neg(\exists v \mid 0 \leq v : d \cdot v = p))$

(c) $(\forall x, y{:}\mathbb{Z} \mid (\exists i, j{:}\mathbb{Z} \mid : x = 2 \cdot i + 1 \ \wedge \ y = 2 \cdot j + 1) : (\exists k{:}\mathbb{Z} \mid : x + y = 2 \cdot k))$

English to predicate logic

9.35 Formalize the following English sentences in predicate logic.

(a) You can fool some of the people some of the time.

(b) You can fool all the people some of the time.

English to predicate logic

9.35 Formalize the following English sentences in predicate logic.

(a) You can fool some of the people some of the time.

(b) You can fool all the people some of the time.

9.35 Define

$$fool(p,t): \text{ You can fool person } p \text{ at time } t.$$

Let P be the set of all people. Let time be modeled as the integers (seconds, say), starting at some initial time 0.

(a) $(\exists p{:}P \mid : (\exists t{:}\mathbb{N} \mid : fool(p,t)))$

(b) $(\forall p{:}P \mid : (\exists t{:}\mathbb{N} \mid : fool(p,t)))$

Any Questions?